AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The person of Scott Andrew Lawrence and the premises located at 8687 SE Ellis St., Portland, Oregon 97266, more fully described in Attachment A

Case No. '19 -MC- 879

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The person of Scott Andrew Lawrence and the premises located at 8687 SE Ellis St., Portland, Oregon 97266, more fully described in Attachment A hereto.

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 2251(a)	Production of Child Pornography
18 USC 2252A(a)(2), (a)(5)(B)	Receipt, Distribution, and Possession of Child Pornography

The application is based on these facts:

See the attached affidavit of FBI Task Force Officer Nathan A. Tobey.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

11:00 a.m.

Applicant's signature

Nathan A. Tobey, Task Force Officer, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/21/2019

John D Russo

Judge's signature

City and state: Portland, Oregon

Hon. Jolie Russo, United States Magistrate Judge

Printed name and title

STATE OF OREGON)
) ss. AFFIDAVIT OF NATHAN A. TOBEY
County of Multnomah)

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Nathan A. Tobey, being duly sworn, hereby depose and state as follows:

Introduction

1. I am a Detective employed by the Portland Police Bureau and have been so employed since December 1998. I am also a Task Force Officer with the Federal Bureau of Investigation (FBI) and have been so assigned since November 2018. I am currently assigned to the Portland Division of the FBI where I investigate computer-related crimes. I have received training in the investigation of computer, telecommunications, and other technology crimes. Since November 2018, I have been involved in the investigation of matters involving the sexual exploitation of children, including the online sexual exploitation of children, in violation of Title 18, United States Code (U.S.C.), Sections 2251, 2252A, and 2422. I am part of the Child Exploitation Task Force (CETF), which includes FBI Special Agents and Task Force Officers. CETF is an intelligence-driven, proactive, multi-agency investigative initiative to combat the proliferation of child pornography/child sexual exploitation facilitated by an online computer and other aspects of child exploitation.

2. I submit this affidavit in support of an application for a warrant to search the person of SCOTT ANDREW LAWRENCE, a Caucasian male born XX/XX/1964 who stands approximately 5'9" tall and weighs approximately 210 pounds, and his residence located at 8687 SE Ellis Street, Portland, Oregon 97266, further described in Attachment A, for contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections

2251(a), 2252A(a)(2); and 2252A(a)(5)(B), which prohibit the production, receipt, distribution, and possession of child pornography. I have probable cause to believe that such items, further described in Attachment B, are currently located on LAWRENCE's person and in his residence.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The statements contained in this affidavit are based upon the following: my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience.

Applicable Law

4. a. 18 U.S.C. § 2251(a) makes it unlawful to knowingly employ, use, persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct or transmitting a live visual depiction of such conduct, if the defendant knows or has reason to know the visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or if the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce.

b. 18 U.S.C. § 2252A(a)(2)(A) makes it a crime to knowingly receive or distribute child pornography using any means or facility of interstate or foreign commerce, or that has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

c. 18 U.S.C. § 2252A(a)(5)(B) makes it a crime to knowingly possess or access with intent to view child pornography that has been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that were mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer. The term "child pornography" is defined in 18 U.S.C. § 2256(8).

Background on Computers and Child Pornography

5. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have drastically changed the manner in which child pornography is produced and distributed.

6. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage.

7. Child pornographers can upload images or video clips directly from a digital camera to a computer. Once uploaded, they can easily be edited, manipulated, copied, and distributed. Paper photographs can be transferred to a computer-readable format and uploaded to a computer through the use of a scanner. Once uploaded, they too can easily be edited, manipulated, copied, and distributed. A modem allows any computer to connect to another

computer through the use of a telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

8. The computer's ability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Images and videos of child pornography can also be stored on removable data storage media, such as external hard drives, thumb drives, media cards, and the like, many of which are small and highly portable and easily concealed, including on someone's person.

9. The Internet affords collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion, including Internet Relay Chat, instant messaging programs, bulletin board services, e-mail, social media, and "peer-to-peer" (P2P) file sharing programs such as LimeWire, eMule, and networks such as Gnutella and BitTorrent, among others. Collectors and distributors of child pornography also use online resources such as "cloud" storage services to store and retrieve child pornography. Such online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer.

10. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example,

by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in the computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains P2P software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

11. Social media platforms, such as Facebook and Instagram, afford users the opportunity to create unique profiles and communicate publicly and privately with other users. Users can share image and video files privately on social media. With respect to child pornography investigations, suspects will often induce or entice people they know to be children to produce sexually explicit images or videos of themselves and send those files to the suspect via social media. Suspects use a variety of methods to save the images and video files they receive, including saving them directly from the social media platform to their device, taking screenshots of the received files, and using screen recording applications to capture the files.

12. I know based on my training and experience, and based on conversations I have had with others who investigate child exploitation offenses, that people who have a sexual interest in children, including persons who collect and trade in child pornography, often receive sexual gratification from images and video clips depicting the sexual exploitation of children. They may also use such images and videos to lower the inhibitions of children who they wish to sexually abuse. Such persons maintain their collections of child pornography in safe, secure, and

private locations, such as their residence, and on computers and digital storage media under their direct control. Such persons often maintain their collections, which are considered prized possessions, for long periods of time, and prefer not to be without their collections for any prolonged period of time. In some recent cases, however, some persons with a sexual interest in children have been found to download and delete child pornography on a cyclical and repetitive basis, rather than storing a collection of child pornography indefinitely.

13. I know based upon my training and experience that mobile devices, such as smartphones and tablet computers, have in many cases replaced traditional computers for many people. I read an amicus brief submitted to the United States Supreme Court in the case entitled *David Leon Riley v. State of California*, which involved the search of a mobile device. The brief was titled "Brief of the National Association of Criminal Defense Lawyers and the Brennan Center for Justice at New York University School of Law as Amici Curiae in Support of Petitioner." The brief discussed the habits of mobile device users and reliance people have on their mobile devices. A section of the brief reads:

> "Unlike virtually any other technology, mobile devices have become an extension of one's self, completely integrated into daily living. Seventy-two percent of smartphone owners keep their phone within an arm's reach at all times. Jumio, *Mobile Comsumer Habits 2013 Study.* Sixty-five percent of all cell phone owners actually sleep with their phone. Amanda, Lehart, *Cellphones and American Adults 11 (2010).* A 2012 survey found 58% of phone owners check their phones at least once an hour, in bed before sleep and immediately upon waking. Haris Interactive, *Mobile Mindset Survey (2012).* Over 50% use their phone while driving, nearly 20% use their phone during church, and 12% continue to use their phone in the shower. Jumio, supra.
>
> "The mobile computing revolution has created a virtual digital life that exists alongside and parallel to a physical life. Modern society now lives both simultaneously, with each being integral to work, family, love and daily living. And our mobile devices are the doorway to our virtual homes."

14. I know from my training and experience, from having an understanding of a person's mobile device use as referenced in the quoted brief above, and from my experience as an investigator, that a person with a sexual interest in children will likely have evidence of child pornography on their mobile device. In 2016, I became a Cellebrite Certified Logical Operator and a Cellebrite Certified Physical Analyst, and as such, I am qualified to extract data from mobile devices using Cellebrite technology. Cellebrite is a company that has developed software and technology to facilitate the extraction, decryption, and parsing of data from mobile devices. Since becoming certified by Cellebrite, I have extracted data from over 100 mobile devices, the majority of which involved cases where the person was suspected of having child pornography stored on their mobile device. I know from my training and experience that a person's mobile device will likely be found on their person, in their vehicle, and in their residence.

15. I know from my training and experience that mobile devices can be backed up to computers. I have personally seen in many cases I have investigated that people transfer data from their mobile devices to their computers as a way to backup and preserve the data on their mobile phone. I know that a thorough investigation of child pornography crimes requires law enforcement to seize computers, not only for the reasons listed above, but also because the mobile device backups can be recovered, decrypted, and parsed by computer forensic examiners. The data from mobile backups is useful and relevant in an investigation of child pornography.

Statement of Probable Cause

16. On September 12, 2019, I reviewed CyberTipline Report 54667233, which Facebook submitted to the National Center for Missing and Exploited Children. Facebook employees reported sexually explicit communication between LAWRENCE and a 16-year-old

boy, identified herein as Minor Victim 1 (MV1). MV1, who was born in 2003, lives in Centerville, South Dakota. I also reviewed information contained in CyberTipline Reports 51351158 and 54391204, which were also initiated by Facebook and are related to this investigation.

17. CyberTipline Report 54667233 was initially sent to and investigated by the Oregon Department of Justice (ODOJ). Facebook provided several recent IP Addresses associated with LAWRENCE's Facebook account. One of those IP Addresses was 2601:01c2:0680:1f5a:95cd:b6c1:0d41:412a. ODOJ researched that IP Address and discovered it was serviced by Comcast. ODOJ sent an administrative subpoena to Comcast to obtain subscriber information for the IP Address. In response to the subpoena, Comcast identified the service address for the IP Address as 8687 SE Ellis Street, Portland, OR 97266. ODOJ forwarded the investigation to the Portland Police Bureau, who assigned it to me.

18. On September 19, 2019, I applied for and received an Oregon state search warrant for records and content from the Facebook profiles belonging to LAWRENCE and MV1. I served the warrant on Facebook that same day. On September 24, 2019, I downloaded responsive data from Facebook. I examined the data from LAWRENCE's and MV1's Facebook accounts for evidence relevant to this investigation.

Evidence of Attribution (Scott Lawrence Facebook Profile)

19. LAWRENCE's Facebook profile had numerous data points indicating that LAWRENCE created, accessed, and used the profile. LAWRENCE used the name "Scott Lawrence" when he created the account. He listed his actual date of birth in his Facebook profile.

20. In response to the warrant, Facebook provided the photos stored on LAWRENCE's profile. Two images were stored in "Profile pictures." The first photo was uploaded on 4/10/2019. The second was uploaded on 4/21/2019. Both photos clearly show LAWRENCE's face. Both depict the same person shown in LAWRENCE's Oregon driver's license photograph.

21. LAWRENCE also sent photographs of himself to various people during private Facebook messages with those people. Examples follow.

a. On 4/19/2019, LAWRENCE sent a picture of himself to Sheila Mae Fuentespina that showed LAWRENCE wearing a blue "Arizona" sweatshirt and a hat. LAWRENCE's face was visible in the picture. LAWRENCE followed up with a message to FUENTESPINA saying, "See how I look."

b. On 5/8/2019, LAWRENCE sent a picture of his Polk County Jail Inmate Identification Card to Fuentespina during a Facebook chat. Fuentespina asked LAWRENCE to send her money; LAWRENCE sent her a picture of his inmate ID card and said he had other financial obligations. The inmate identification card had LAWRENCE's face, full name, physical description, and date of birth on it.

c. On 5/27/2019, LAWRENCE sent another picture of himself to Fuentespina. The picture showed LAWRENCE's face. In the picture LAWRENCE was wearing a black coat, gray shirt, reading glasses, and a hat with the number "3" on it.

d. On 6/14/2019, LAWRENCE sent a picture of himself to Seen Lang during a private chat. The picture showed LAWRENCE's face. In the picture, LAWRENCE wore black rimmed glasses and a dark shirt, and was leaning against a green colored wall.

e. On 5/29/2019, LAWRENCE sent a picture to Brooke Vanhook. The picture was a side-by-side image. One half of the image showed a man's erect penis with ejaculate coming out of it; the other half showed LAWRENCE's face. In the half depicting LAWRENCE's face, he is wearing dark rimmed glasses and headphones.

f. On 6/23/2019, LAWRENCE sent a picture of himself to a minor female identified herein by the initials "BJ" during a Facebook chat conversation. The image showed LAWRENCE's face. LAWRENCE wore a black tank top; tattoos are visible on both of his shoulders. During the chat, BJ identified herself as a 14 year-old girl from England. LAWRENCE was sexually explicit during the conversation.

Phone Evidence of Attribution

22. LAWRENCE had a private Facebook conversation with Joannester Albrecht on 5/2/2019. During the conversation, Albrecht asked LAWRENCE for his phone number. LAWRENCE replied that it is "971-252-0428." That is the phone number LAWRENCE listed when he created his Facebook profile. That phone number is serviced by T-Mobile. ODOJ sent an administrative subpoena to T-Mobile to obtain subscriber records pertaining to the phone number and to an IP address associated with LAWRENCE's Facebook activity. The records showed that the T-Mobile account belonged to Nicole Hughes. The device assigned to that account is a Moto E5 Play. That account was closed on 5/10/2019.

23. In LAWRENCE's chat conversations he repeatedly talked about "Nicole" with a person named Clifford Frey. FREY identified "Nicole" as his girlfriend. On 6/2/2019, LAWRENCE and Frey had the following exchange which appeared to be regarding LAWRENCE's phone:

FREY: I talked with Nicole an she admit the number did get taken

LAWRENCE: Why

FREY: She told me it was when the phone got shout off when it was supposed until she paid the 104

24. I reviewed records maintained by a Portland area regional law enforcement database, which is called "RegJin." RegJin listed Nicole Hughes as having a home address of 1836 SE 151st Ave, Portland, OR 97233. RegJin also lists Hughes as Frey's girlfriend.

25. RegJin records showed that Frey is a registered sex offender. Frey had a registered address of 8687 SE Ellis Street, Portland, OR. Facebook communications between Frey and LAWRENCE suggest that they were roommates at that address. Based upon their Facebook communications, it appears LAWRENCE obtained a phone belonging to Nicole Hughes based on his connection with Frey.

26. During his chat conversation with Frey, LAWRENCE sometimes assumed the identity of a female. When he did that, the female persona claimed that LAWRENCE was somewhere else and that "she" was using LAWRENCE's Facebook account to chat with Frey. LAWRENCE sent sexually explicit images of women to Frey while purporting to be a woman, and asked Frey to send pictures of himself masturbating. LAWRENCE employed that same tactic with MV1.

Sexually Explicit Communication Between Lawrence and MV1

27. The Facebook records contained private chat conversations between LAWRENCE and MV1. Transcripts of the conversation matched what Facebook provided in

the CyberTipline Report. The records included additional text that was not included in the original CyberTipline Report.

28. LAWRENCE used a ruse to trick MV1 into believing he was talking to a female. LAWRENCE called himself "Mary" and told MV1 that "she" could only communicate with him via LAWRENCE's Facebook account. Posing as "Mary," LAWRENCE sent sexually explicit images of different women to MV1 to get MV1 sexually aroused. LAWRENCE then convinced MV1 to produce and send sexually explicit images and videos of himself masturbating to LAWRENCE's Facebook account.

29. LAWRENCE, posing as "Mary," requested sexually explicit images of MV1 on multiple days. On at least three separate days, MV1 complied with "Mary's" request, and sent sexually explicit images of himself to LAWRENCE via Facebook Messenger.

30. LAWRENCE knows that MV1 is a child. On 6/16/2019, LAWRENCE sent MV1 a message that read, "Your 15 now right." MV1 replied, "No 16." LAWRENCE then had a sexually explicit conversation with MV1 after clarifying MV1's age.

31. MV1 first sent sexually explicit videos to LAWRENCE on 6/16/2019. MV1 sent two video files showing himself masturbating. MV1 deleted the video files after sending them. Nonetheless, Facebook captured the files, included them in the CyberTipline Report, and provided them in response to the search warrant.

32. The first video file is a close up of MV1 masturbating. MV1 is wearing silver pants or shorts that are pulled down to reveal his penis. The video was 20 seconds long. The second video, which appears to be a continuation of the first video, is also 20 seconds long. It is

also a close up of MV1 masturbating. At the end of the second video, MV1 ejaculated on his hand.

33. During the chat conversation that led to MV1 sending the two videos, LAWRENCE posed as "Mary." LAWRENCE sent MV1 sexually explicit images of women to get him sexually aroused. "Mary" then requested that MV1 record himself masturbating and send the images to him. That conversation follows:

LAWRENCE:	Are you in your bunk
MV1:	Yea
LAWRENCE:	Take your dick out
LAWRENCE:	*Sent image of nude woman on bed with her legs spread and her hand touching her exposed vagina*
MV1:	It is
LAWRENCE:	Like my pussy
MV1:	Yea
LAWRENCE:	Are you jacking off
MV1:	Not yet
LAWRENCE:	Want more
MV1:	Yea
LAWRENCE:	Start jacking off and take video of you doing it
LAWRENCE:	*Sent close up image of woman's exposed anus and vagina*
LAWRENCE:	*Sent close up image of woman's exposed vagina*
LAWRENCE:	That's my pussy

MV1:	Ok
LAWRENCE:	Stick your dick in me
LAWRENCE:	Send video
MV1:	Ok
LAWRENCE:	*Sent close up of a woman touching her vagina with her fingers*
LAWRENCE:	Jacking off
MV1:	Yea
LAWRENCE:	Video your cum
MV1:	Yea
LAWRENCE:	Squirt
MV1:	Ok
LAWRENCE:	Show me
MV1:	I'm trying to get my camera to work
LAWRENCE:	Ok
LAWRENCE:	Cum baby squirt in my mouth
LAWRENCE:	Fill my mouth
MV1:	*Sent thumbs up emoji*
LAWRENCE:	I will swallow your sperm
MV1:	Huh
LAWRENCE:	I want your cum are you close
MV1:	Yea
LAWRENCE:	Show me your dick

MV1:	*Sent first video described above* (Deleted video 4.5 minutes after sending it)
MV1:	*Sent second video described above* (Deleted 3.5 minutes after sending it)
LAWRENCE:	Nice baby. IAM going to masterbate to your cum and I will send to cindy
MV1:	Ok
LAWRENCE:	Hey
MV1:	Hey
LAWRENCE:	You removed the video
MV1:	Where is Scott now and sorry...wrong g one
LAWRENCE:	Re send Scott is at work
MV1:	I now that....I'm trying to resend them I cant find them
LAWRENCE:	Scott has seen your dick and touch it once on accedent before that lady came inside
MV1:	Yea
LAWRENCE:	He told me you have a really nice dick
MV1:	YeA
LAWRENCE:	Yes he liked it
MV1:	Yea
MV1:	I cant find them
LAWRENCE:	He told me he would jack you off in front of me

MV1:	Ok
LAWRENCE:	I think when we play it should be you and Scott and i
MV1:	Ok
LAWRENCE:	Can Scott play with you too
MV1:	Yeah!
LAWRENCE:	I want Scott to jack you off in my mouth. And you jack Scott off in my mouth
MV1:	Ok
LAWRENCE:	You like Scott don't you
MV1:	Yea
LAWRENCE:	Yes he likes you. Aot
MV1:	Yea
LAWRENCE:	He really wanted to taste your dick and cum
MV1:	Ok
LAWRENCE:	I think you would let him
MV1:	Yea
LAWRENCE:	Would you do that to him
MV1:	Yeah!
LAWRENCE:	He told me you made him hard alot
MV1:	Ok
LAWRENCE:	Do you ever think about scott
MV1:	Yeah!

LAWRENCE: When the three of us go out. Can I watch you and Scott suck each other

MV1: I'm good on that one

LAWRENCE: Can I watch Scott suck you while you eat my pussy

MV1: Yea

MV1: Does cindy have a phone

LAWRENCE: Cindy text me she was asking about the video and i told her you accedently erased them

MV1: Ok I all can redo tommor or sometime but I cant do them tommor night bc we ate getting unloaded

LAWRENCE: That's fine hun. I told her you have nice cum

MV1: Ok

LAWRENCE: We can have Cindy with use to. You can fuck me and Scott can fuck Cindy then we can trade

MV1: Yea

LAWRENCE: Where can we get a motel room at

MV1: Bearford where I work at but over the intersection Scott know where its at

34. The conversation continued with LAWRENCE asking MV1 what sex acts he would be willing to perform with LAWRENCE and the fictitious girls when they all got together. LAWRENCE discussed how different foods affected the taste of semen and the age at which MV1 first masturbated.

35. On 6/17/2019, MV1 and LAWRENCE had a second sexually explicit chat conversation during which MV1 sent LAWRENCE a single still image and two video files of himself masturbating at LAWRENCE's request. The still image was a close-up photograph of a hand holding MV1's erect penis. MV1 was concealing his penis under a blanket. Law enforcement officers in South Dakota spoke with MV1 and confirmed that the image depicted MV1's penis. The two video files were both 20 seconds in length and showed LAWRENCE's exposed penis with him masturbating. The second video showed LAWRENCE ejaculating. MV1 was wearing bright blue shorts in the two videos that were pulled down to show his erect penis.

36. The conversation on 6/17/2019 leading up to MV1 sending the image and video files follows.

LAWRENCE:	*Sent image of nude adult woman in bathtub with her legs spread to show her vagina and exposed breasts*
LAWRENCE:	*Sent image of close up of woman's exposed vagina and anus*
LAWRENCE:	*Sent image of close up of woman's exposed vagina. Woman was using her fingers to open her vagina*
LAWRENCE:	Getting hard
MV1:	Yeah
LAWRENCE:	Lick me [MV1's first name] and let Scott suck you
MV1:	Om
MV1:	Ok
LAWRENCE:	Do I taste good

MV1:	Yra
LAWRENCE:	Is Scott sucking your dick good
MV1:	Yea
LAWRENCE:	Are you hard
MV1:	Yea
LAWRENCE:	Yes [MV1's first name] cum in Scott's mouth
MV1:	Ok
LAWRENCE:	Are you on your bunk
MV1:	Yes
LAWRENCE:	Jack off
MV1:	Ok
LAWRENCE:	I bet your dick feels good
MV1:	Yea
LAWRENCE:	Show me now
LAWRENCE:	*Sent image of woman's exposed vagina with ejaculate on the outside of her vagina*
LAWRENCE:	Scott's cum around my pussy
MV1:	Yea
MV1:	*Sent image described above*
LAWRENCE:	Cum please video it
MV1:	Ik
MV1:	.ik

LAWRENCE:	Squirt baby
MV1:	Ok
MV1:	*Sent video file* (Sent 6/17/2019 at 22:06:10 PDT)
MV1:	*Sent video file* (Sent 6/17/2019 at 22:06:56 PDT)
LAWRENCE:	Nice [MV1's first name]
MV1:	Yep
LAWRENCE:	Now don't earase them yet
MV1:	Ok
LAWRENCE:	Fee better
MV1:	I erased them from my phone and yea
LAWRENCE:	Ok I got them. If you want earase from your phone

37. LAWRENCE and MV1 had a third sexually explicit conversation on 6/22/2019 during which MV1 sent sexually explicit videos of himself to LAWRENCE at LAWRENCE's request. The chat followed the same pattern as the two previously described conversations. LAWRENCE purported to be a female and he sent sexually explicit images of women to MV1 for the purpose of sexually arousing MV1. The two video files MV1 sent during this chat conversation both depicted MV1 masturbating. MV1 appeared to be trying to conceal himself with a blanket. The videos were each 20 seconds long. The first video showed MV1 masturbating. The second video showed MV1 masturbating then ejaculating on his stomach. These videos were distinguishable from the videos sent on 6/16/2019 and 6/17/2019 because MV1 did not appear to be wearing any pants or shorts in the videos.

38. LAWRENCE communicated with MV1 as himself on at least one occasion. During that conversation LAWRENCE claimed that he heard from "Mary" that MV1 was open to having sexual contact with him. LAWRENCE discussed various sex acts with MV1 to see what MV1 would be comfortable doing when they got together. The conversation, which began on 6/18/2019, follows:

LAWRENCE:	Cindy loves your dick and especially your cum
MV1:	Yea I kinda figured she would
LAWRENCE:	Yes you guys are going to get alone
MV1:	Ok
MV1:	Must be Scott
LAWRENCE:	Hell yes son
LAWRENCE:	I liked it too
MV1:	Ok I was checking
LAWRENCE:	Want to talk to me
LAWRENCE:	I wish you would of told me
MV1:	Yea heavt talked to u for a while
MV1:	Oh sorry
LAWRENCE:	Yes been busy local
MV1:	Yea we been busy to we been out on the road for a month now
LAWRENCE:	Is you dad getting payed
MV1:	Yea
LAWRENCE:	That's good

MV1:	Yea
LAWRENCE:	I really wanted to suck you when I lived there
MV1:	Oh
LAWRENCE:	Mary told me you thought the same thing
MV1:	Yea
LAWRENCE:	That would of been fun
MV1:	Yea
LAWRENCE:	I would of let you cum in my mouth
MV1:	Ok
LAWRENCE:	Do you want to jack me off
MV1:	Yes
LAWRENCE:	Do you want to see my cum
MV1:	Sure
LAWRENCE:	Can I cum on you
MV1:	Na I'm good
LAWRENCE:	Ok you have to tell me so I know
MV1:	Ok

Victim Identity and Image Confirmation

39. Special Agent Kendra Russell with the South Dakota Division of Criminal Investigations assisted with this investigation and contacted MV1's family. SA Russell identified MV1, confirmed he was born in 2003, and confirmed that he lived in Centerville, South Dakota. SA Russell met with MV1 on September 27, 2019. MV1 confirmed that the still

image file was a picture of MV1's penis. MV1 told her he sent image and videos to LAWRENCE.

40. SA Russell learned that LAWRENCE lived with MV1's family for about six months approximately a year and a half ago. MV1 told her that LAWRENCE never touched him inappropriately. MV1 was uncomfortable discussing this case, and repeatedly tried to change the topic.

Distribution of Victim's Sexually Explicit Image

41. I found at least two instances in which LAWRENCE distributed a sexually explicit image of MV1 to another person via Facebook. In both instances it was the image of MV1's erect penis in MV1's hand that MV1 sent to LAWRENCE on 6/17/2019.

42. On 6/18/2019, LAWRENCE was having a private Facebook chat conversation with a user whose user name is "Mudasir Khan." LAWRENCE sent the image of MV1 to Khan after greeting him with "Hi baby." LAWRENCE did not discuss the origin of the image or provide any identifying information about MV1.

43. Also on 6/18/2019, LAWRENCE sent the image of MV1's penis to a Facebook user with the user name "Seen Lang." LAWRENCE and Lang had been having a sexually explicit conversation in the preceding days. LAWRENCE did not provide any identifying information about MV1 when he sent the image to Lang.

Relevant IP Address History

44. I reviewed the relevant IP address history Facebook provided for LAWRENCE's account. The IP addresses varied somewhat. I focused on IP addresses used to access LAWRENCE's Facebook account between 6/16/2019 and 6/22/2019. I compared the IP address

history provided by Facebook with the IP address records provided by Comcast and I determined all of the IP addresses used to access LAWRENCE's Facebook account during that time period were assigned to the Comcast account at 8687 SE Ellis Street, Portland, OR 97266.

LAWRENCE's Sex Offender Status and Address Confirmation

45. I queried files maintained by the Law Enforcement Data System (LEDS) and National Crime Information Center (NCIC) and I learned that LAWRENCE is a registered sex offender. LAWRENCE was convicted in California in 2001 of continuous sexual abuse of a child and lewd or lascivious acts with a child under 14 years of age. LAWRENCE was sentenced to 14 years in prison. As a result of that conviction, LAWRENCE is required to register as a sex offender while living in the State of Oregon. LAWRENCE is registered at 8687 SE Ellis Street, Portland, OR 97266.

46. On September 25, 2019, Portland Police Officer Samantha Wuthrich went to LAWRENCE's residence to confirm that he was actually living at his registered address. Officer Wuthrich spoke with LAWRENCE at the residence. He showed her his bedroom, which she described as a closet in the basement of the residence next to the laundry room. Officer Wuthrich told me the residence is a clean and sober living home. Several other people live there as well.

47. The residence is a cream colored multi-level home located on the northwest corner of SE Ellis Street and SE 87th Avenue. It has white trim and maroon shutters. The front door is white. The numbers "8687" are affixed in two places – next to the front door, and on the south side of the house.

Search and Seizure of Digital Data

48. This application seeks permission to search for particular items, described in Attachment B, which will likely be found on SCOTT LAWRENCE's person and in his residence, in whatever form those items may be found. One form in which that evidence will likely be found is as data stored on a computer's hard drive, on other digital storage media, or on other digital devices, including cell phones. Thus, the warrant applied for would authorize the seizure of electronic storage media or the copying of electronically stored information, all under Fed. R. Crim. P. 41(e)(2)(B).

49. I have probable cause to believe that the items described in Attachment B will be stored on one or more digital device(s), based on the foregoing facts and on my knowledge, training, and experience that:

a. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the digital device until it is overwritten by new data. Therefore, deleted files or remnants of deleted files may reside in free space or slack space – that is, in space on the digital device that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Wholly apart from user-generated files, digital devices – in particular, internal hard drives – contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. For example, forensic evidence can take the form of operating system configurations, artifacts from the operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant but also forensic electronic evidence that establishes how digital devices were used, the purpose of their use, who used them, and when. I have probable cause to believe that this forensic electronic evidence will be on any digital device in SCOTT LAWRENCE's possession, in his vehicle, or in his residence, because, based on my knowledge, training, and experience, I know:

a. Data on a digital device can provide evidence of a file that was once on the digital device but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the digital device that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of

peripherals, the attachment of USB flash storage devices or other external storage media, and the times the digital device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, email, email address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. In addition, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device, or password-protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the digital device and the application of knowledge about how a digital device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a digital device. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a digital device to commit a crime such as the child pornography offenses described herein, the individual's digital device will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The digital device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The digital device is also likely to be a storage medium for evidence of the crime. From my training and experience, I believe that a digital

device used to commit a crime of this type may contain data that is evidence of how the digital device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

51. In most cases, a thorough search of premises for information that might be stored on a digital device often requires the seizure of the device and a later, off-site review consistent with the warrant. In lieu of removing a digital device from the premises, it is sometimes possible to image or copy it. Generally speaking, imaging is the taking of a complete electronic picture of the digital device's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the digital device and to prevent the loss of the data either from accidental or intentional destruction. This is true because:

a. Not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a digital device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine digital devices to obtain evidence. Digital devices can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Records sought under this warrant could be stored in a variety of formats that may require off-site reviewing with specialized forensic tools. Similarly, digital devices can

be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the digital device off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

52. Because it appears that at least one other person resides at the premises, it is possible that the premises will contain digital devices that are owned and/or predominantly used by persons who are not suspected of a crime. I am requesting authorization to search only those devices belonging to or that were used or accessed by Scott LAWRENCE. I am not seeking authorization to seize or search devices belonging to other people that LAWRENCE neither used nor had access to.

53. *Nature of the examination.* Based on the foregoing, and consistent with Fed. R. Crim. P. 41(e)(2)(B), the warrant for which I am applying would permit seizing, imaging, or otherwise copying digital devices that reasonably appear to contain some or all of the evidence described in the warrant and Attachment B, and would authorize a later review of the device or information consistent with the warrant. The later review may require techniques, including computer-assisted scans of the entire device that might expose many parts of a hard drive to human inspection in order to determine whether it contains material subject to seizure and search under the warrant.

54. The initial examination of the digital device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of that time period from the Court.

55. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the digital device do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

56. If an examination is conducted, and the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search and will seal any image of the digital device, absent further authorization from the Court.

57. The government may retain any digital device containing contraband or evidence, fruits, or instrumentalities of the offenses described above and in Attachment B, or to commence forfeiture proceedings against the device and/or the data contained therein.

58. The government will retain a forensic image of the digital device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

59. The government has not made any prior efforts in other judicial fora to obtain the evidence sought under the warrant.

Conclusion

60. Based on the foregoing information, I have probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251(a), 2252A(a)(2), and 2252A(a)(5)(B), as set forth herein and in Attachment B, are currently on SCOTT LAWRENCE's person and in areas of his residence (including storage areas), described in Attachment A, to which he has access or over which he exercises dominion or control. I therefore respectfully request that the Court issue a warrant authorizing searches of SCOTT LAWRENCE's person and areas of his residence for the items described above and in Attachment B, and authorizing the seizure and examination of any such items found.

///

///

///

61. This affidavit, the accompanying application, and the requested search warrant were reviewed by Assistant United States Attorney Gary Sussman prior to being submitted to the Court. AUSA Sussman informed me that in his opinion, the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

NATHAN A. TOBEY
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me this 21 day of October 2019.

HONORABLE JOLIE RUSSO
United States Magistrate Judge

ATTACHMENT A

Description of Person to be Searched

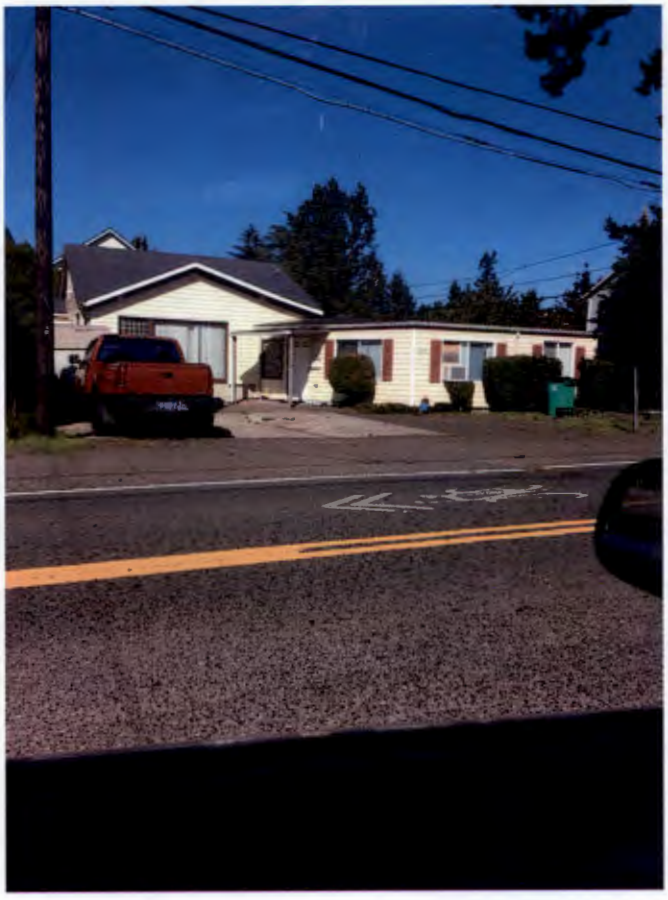
SCOTT ANDREW LAWRENCE, a 55 year old Caucasian male, date of birth XX/XX/1964, standing approximately 5'9" tall, weighing approximately 210 pounds.

Description of Location to be Searched

The Premises Located at 8687 SE Ellis Street, Portland, Oregon 97266

A cream colored multi-level home located on the northwest corner of SE Ellis Street and SE 87th Avenue. The house has white trim with maroon shutters. The front door is white. The numbers "8687" are affixed in two places – next to the front door, and on the south side of the house.

This warrant authorizes searches of common areas of the residence (the kitchen, dining room, living room, bathroom, and the like), and any areas of the premises (including storage areas) accessed by or accessible to SCOTT ANDREW LAWRENCE, and any areas under his dominion or control.



ATTACHMENT B

Items to Be Seized

The following items, records, documents, and materials that constitute or contain contraband or evidence, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2), and 2252A(a)(5)(B) (production, receipt, distribution, and possession of child pornography).

1. Items to be searched for, seized, and examined:

a. All records, documents, or materials, including correspondence, pertaining to the production, transportation, distribution, receipt, possession of, or accessing with intent to view child pornography, as that term is defined in 18 U.S.C. § 2256;

b. All originals and copies of visual depictions of minors engaging in sexually explicit conduct as that term is defined in 18 U.S.C. § 2256, including photographs, images, and videos, whether in physical or digital form;

c. Computers, storage media, or digital devices, including cellular telephones, that are owned by Scott Andrew LAWRENCE, were accessed or used by him, or are capable of being used by him to commit the offenses described above, or to create, access, or store contraband or evidence, fruits, or instrumentalities of those offenses;

d. Evidence of internet usage for the production of, transportation of, receipt or distribution of, possession of, or accessing with intent to view child pornography as defined in 18 U.S.C. § 2256, including dates and times of usage; IP addresses; and

screennames, user names, and passwords used to access the internet or any accounts via the internet;

e. Communications, including emails, chats, bulletin board posts, and comments relating to the production, transportation, distribution, receipt, possession of, or accessing with the intent to view child pornography, to children engaged in sexually explicit conduct, and/or to a sexual interest in children;

f. All records, documents, or materials naming or identifying minors visually depicted while engaging in sexually explicit conduct, as that term is defined in 18 U.S.C. § 2256.

2. As used in this attachment, the terms "records," "items," "documents," and "materials" include all of the foregoing items in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant and any computer, storage medium, or digital device that contains, is capable of containing, or in which is stored records or information that is otherwise called for by this warrant (hereinafter "Computer"):

a. Evidence of who used, owned, or controlled the Computer at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence.

b. Evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software.

c. Evidence of the lack of such malicious software.

d. Evidence indicating how and when the Computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime under investigation and to the Computer user.

e. Evidence indicating the Computer user's state of mind as it relates to the crime under investigation.

f. Evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence.

g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer.

h. Evidence of the times the Computer was used.

i. Passwords, encryption keys, and other access devices that may be necessary to access the Computer.

j. Documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer.

k. Records of or information about Internet Protocol addresses used by the Computer.

l. Records of or information about the Computer's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

m. Contextual information necessary to understand the evidence described in this attachment.

n. Routers, modems, and network equipment used to connect computers to the Internet.

Search Procedure

4. The search for data capable of being read, stored, or interpreted by a computer or storage device may require authorities to employ techniques, including imaging any computer or storage media and computer-assisted scans and searches of the computers and storage media, that might expose many parts of the computer to human inspection in order to determine whether it constitutes evidence as described by the warrant.

5. The initial examination of the computer and storage media will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the computer and storage media do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders

further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

7. If an examination is conducted and the computer and storage media do not contain any data falling within the ambit of the warrant, the government will return the computer and storage media to its owner within a reasonable period of time following the search and will seal any image of the computer and storage media, absent further authorization from the Court.

8. The government may retain any digital device containing contraband or evidence, fruits, or instrumentalities of the offense described herein, or to commence forfeiture proceedings against the computer and storage media and/or the data contained therein.

9. The government will retain a forensic image of the computer and storage media for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering with, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.